COMPLETE SET OF CLAIMS

1   1.   (Currently Amended) An authentication communication system which includes

2   (a) a storage medium having an area for storing digital information and (b) an access device for

3   reading/writing digital information from/into the area, the authentication communication system

4   comprising:

5   a first authentication phase in which the access device transmits to the storage

6   medium scrambled access information generated by scrambling access information which shows

7   the area, and authenticates whether the storage medium is authorized according to a challenge-

8   response authentication protocol ~~by transmitting scrambled access information generated by~~

9   ~~scrambling access information which shows the area, to the storage medium~~ using the scrambled

10   access information;

11   a second authentication phase in which the storage medium authenticates whether

12   the access device is authorized; and

13   a transfer phase in which, when the storage medium and the access device have

14   authenticated each other as authorized devices, the storage medium extracts the access

15   information from the scrambled access information that was used in the authentication protocol,

16   and the access device reads/writes digital information from/into the area shown by the access

17   information.

18   2.   (Original) The authentication communication system of Claim 1,

19   wherein in the first authentication phase,

20   the access device includes:

21   an access information acquisition unit for acquiring the access information which

22   shows the area;

23   a random number acquisition unit for acquiring a random number;

24   a generation unit for generating random number access information by combining

25   the access information and the random number; and

26   an encryption unit for encrypting the random number access information

27   according to an encryption algorithm, to generate the scrambled access information,

28   the storage medium includes a response value generation unit for generating a

29   response value from the scrambled access information, and

30   the access device includes an authentication unit for authenticating whether the

31   storage medium is authorized using the response value.

32   3.   (Original)   The authentication communication system of Claim 2,

33   wherein in the transfer phase, the storage medium includes:

34   a decryption unit for decrypting the scrambled access information according to a

35   decryption algorithm to obtain the random number access information; and

36   a separation unit for separating the access information from the random number

37   access information.

38   4.   (Original)   The authentication communication system of Claim 3,

39   wherein in the first authentication phase,

40   the access device further includes a random number seed storage unit for storing a

41   random number seed, and

42   the random number acquisition unit acquires the random number by reading the

43   random number seed from the random number seed storage unit.

44   5.   (Original) The authentication communication system of Claim 4,

45   wherein in the first authentication phase, the access device further writes the

46   scrambled access information over the random number seed stored in the random number seed

47   storage unit, as a new random number seed.

48   6.   (Original) The authentication communication system of Claim 3,

49   wherein in the first authentication phase,

50   the access device further includes a random number seed storage unit for storing a

51   random number seed, and

52   the random number acquisition unit acquires the random number, by reading the

53   random number seed from the random number seed storage unit and generating the random

54   number based on the random number seed.

55   7.   (Original) The authentication communication system of Claim 6,

56   wherein in the first authentication phase, the access device further writes the

57   random number over the random number seed stored in the random number seed storage unit as

58   a new random number seed.

59   8.   (Original) The authentication communication system of Claim 3,

60   wherein in the transfer phase,

61   the storage medium, which stores digital information in the area, includes an

62   encryption unit for reading the digital information from the area shown by the access information

63   and encrypting the digital information according to an encryption algorithm to generate

64   encrypted digital information, and

65   the access device, which reads the digital information from the area, includes a

66 decryption unit for decrypting the encrypted digital information according to a decryption

67 algorithm to obtain the digital information, the decryption algorithm being an algorithm for

68 decrypting a cryptogram generated according to the encryption algorithm.

69   9. (Original) The authentication communication system of Claim 3,

70   wherein in the transfer phase,

71   the access device, which writes digital information into the area, includes:

72   a digital information acquisition unit for acquiring the digital information; and

73   an encryption unit for encrypting the digital information according to an

74 encryption algorithm to generate encrypted digital information, and

75   the storage medium includes a decryption unit for decrypting the encrypted digital

76 information according to a decryption algorithm to obtain the digital information, and writing the

77 digital information into the area shown by the access information, the decryption algorithm being

78 an algorithm for decrypting a cryptogram generated according to the encryption algorithm.

79   10. (Original) The authentication communication system of Claim 3,

80   wherein in the transfer phase,

81   the access device, which writes digital information into the area, includes:

82   a digital information acquisition unit for acquiring the digital information;

83   a content key acquisition unit for acquiring a content key;

84   a first encryption unit for encrypting the acquired content key according to a first

85 encryption algorithm to generate an encrypted content key;

86   a second encryption unit for encrypting the encrypted content key according to a

87   second encryption algorithm to generate a double-encrypted content key; and

88   a third encryption unit for encrypting the digital information according to a

89   second encryption algorithm using the content key, to generate encrypted digital information,

90   the storage medium includes a decryption unit for decrypting the double-

91   encrypted content key according to a first decryption algorithm to obtain the encrypted content

92   key, and writing the encrypted content key into the area shown by the access information, and

93   the storage medium further includes an area for storing the encrypted digital

94   information.

95   11.   (Currently Amended) An authentication communication method used in an

96   authentication communication system which includes (a) a storage medium having an area for

97   storing digital information and (b) an access device for reading/writing digital information

98   from/into the area, the authentication communication method comprising:

99   a first authentication step in which the access device transmits to the storage

100   medium scrambled access information generated by scrambling access information which shows

101   the area, and authenticates whether the storage medium is authorized according to a challenge-

102   response authentication protocol ~~by transmitting scrambled access information generated by~~

103   ~~scrambling access information which shows the area, to the storage medium~~ using the scrambled

104   access information;

105   a second authentication step in which the storage medium authenticates whether

106   the access device is authorized; and

107   a transfer step in which, when the storage medium and the access device have

108   authenticated each other as authorized devices, the storage medium extracts the access

109   .information from the scrambled access information that was used in the authentication protocol,

110   and the access device reads/writes digital information from/into the area shown by the access

111   information.

112   12.   (Currently Amended) A computer-readable storage medium which stores an

113   authentication communication program for use in an authentication communication system (a)

114   which includes a storage medium having an area for storing digital information and an access

115   device for reading/writing digital information from/into the area, and (b) in which the digital

116   information is transferred after each of the storage medium and the access device authenticates

117   each other as authorized devices, the authentication communication program comprising:

118   a first authentication step in which the access device transmits to the storage

119   medium scrambled access information generated by scrambling access information which shows

120   the area, and authenticates whether the storage medium is authorized according to a challenge-

121   response authentication protocol by transmitting scrambled access information generated by

122   scrambling access information which shows the area, to the storage medium using the scrambled

123   access information;

124   a second authentication step in which the storage medium authenticates whether

125   the access device is authorized; and

126   a transfer step in which, when the storage medium and the access device have

127   authenticated each other as authorized devices, the storage medium extracts the access

128   information from the scrambled access information that was used in the authentication protocol,

129   and the access device reads/writes digital information from/into the area shown by the access

130   information.

131   13-16. (Cancelled)

132   17.   (New) An access device for reading/writing digital information from/into an area

133   in a storage medium, comprising:

134   authentication means for transmitting to the storage medium scrambled access

135   information generated by scrambling access information which shows the area, and

136   authenticating whether the storage medium is authorized according to a challenge-response

137   authentication protocol using the scrambled access information;

138   proving means for proving to the storage medium that performs authentication of

139   the access device that whether the access device is authorized; and

140   access means for reading and writing digital information from and to the area

141   shown by the access information, which is extracted by the storage medium from the scrambled

142   access information that was used in the authentication protocol, when the storage medium and

143   the access device have authenticated each other as authorized devices.

144   18.   (New) The access device of Claim 17,

145   wherein the authentication means includes:

146   an access information acquisition unit for acquiring the access information which

147   shows the area;

148   a random number acquisition unit for acquiring a random number;

149   a generation unit for generating random number access information by combining

150   the access information and the random number;

151   an encryption unit for encrypting the random number access information

152   according to an encryption algorithm, to generate the scrambled access information; and

153   a transmission unit for transmitting the scrambled access information to the

154   storage medium,

155   the storage medium generates a response value from the scrambled access

156   information, and transmits the response value to the access device, and

157   the authentication means further includes:

158   a reception unit for receiving the response value from the storage medium,

159   and

160   an authentication unit for authentication whether the storage medium is

161   authorized, using the response value.

162   19.   (New) A storage medium having an area for storing digital information wherein

163   an access device reads/writes digital information from/into the area, comprising:

164   proving means for receiving scrambled access information, generated by

165   scrambling access information that shows the area, from the access device and

166   proving whether the storage medium is authorized to the access device that

167   performs authentication of the storage medium according to a challenge-response authentication

168   protocol using the scrambled access information;

169   authentication means for authenticating whether the access device is authorized;

170   and

171   extraction means for extracting the access information from the scrambled access

172   information received by the reception means when the storage medium and the access device

173   have authenticated each other as authorized devices;

174   wherein the access device reads/writes digital information from/into the area

175   shown by the access information extracted by the extraction means.

176   20.   (New) The storage medium of Claim 19,

177   wherein the extraction means includes:

178   a decryption unit for decrypting the scrambled access information according to a

179   decryption algorithm to obtain random number access information; and

180   a separation unit for separating the access information from the random number

181   access information.

1